

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

Middesk, Inc.

Plaintiff,

v.

Osiris Ratings, Inc. d/b/a Baselayer, and

Jonathan Awad, and
Josh Leviloff,

Defendants.

CIVIL ACTION NO. 1:25-cv-02677-PKC

Jury Trial Demanded

REVISED

**PROPOSED ORDER TO PERFORM FORENSIC INSPECTION AND
PROTOCOL AGREEMENT**

WHEREAS on April 15, 2025, the Court heard argument concerning Plaintiff Middesk, Inc.'s ("Plaintiff") Order to Show Cause for Computer Forensics from Defendants Osiris Ratings, Inc. d/b/a Baselayer ("Baselayer") and Jonathan Awad ("Awad") (collectively with "Defendants") (collectively with Plaintiff, referred to as the "Parties"); and

WHEREAS the Parties have agreed to enter into this Protocol ^{cover} covering the below electronic devices and cloud and email accounts:

- Awad's personal Google Drive identified within the Awad Declaration
- Awad's Baselayer Google Drive identified within the Awad Declaration
- Awad's personal email accounts
- Awad's Baselayer email accounts
- Baselayer email accounts that have sent or received data from Awad's personal Google Drive or Baselayer Google Drive
- Awad's personal computer
- Awad's Baselayer computer
- Awad's device(s) and accounts (e.g. social media apps, LinkedIn, WhatsApp, Slack, etc.) used to communicate with Leviloff, including any cell phone and cell phone cloud backups and synchronized data

Having reviewed the submissions of the parties at ECF 51, 53, 56, 58, the Court reverses the Order entered at ECF 50 to provide as follows:

- Leviloff's Baselayer email
- Leviloff's Baselayer computer
- Leviloff's Baselayer Google Drive

WHEREAS, on April 24, 2025, Defendants disclosed that Baselayer Co-Founder Timothy Hyde and Baselayer employee Jared Farber are also administrators of the Baselayer Google Drive that contained Middesk documents. As a result, all computers and phones (business and personal) used by Tim Hyde and Jared Faber shall be added to the devices imaged;

Together, the above devices, accounts, and items are defined as the "Devices".

WHEREAS the Court now orders the following parameters of the forensic review and analysis of the Devices, each of which is set forth in detail in the paragraphs following the Whereas clauses:

- 1) Kroll, LLC, a third-party forensic examiner ("Forensics Examiner") will be engaged by Defendants and Defendants shall cover all costs under this Protocol.
- 2) There will be no substantive ex parte communications with the Forensic Examiner. Plaintiff acknowledges that Defendants may have ex parte communications about purely administrative matters, such as billing and invoicing, with the Forensic Examiner; any ex parte communication with Kroll relating to this forensic examination are discoverable.
- 3) The Forensics Examiner will run searches on the Devices.
- 4) A hit report will be provided to all parties based on those search terms selected solely at Plaintiffs discretion. The Hit Report (as defined below) will be marked attorneys' eyes only HIGHLY CONFIDENTIAL INFORMATION pursuant to the Parties' April 22, 2025 Protective Order.
- 5) Defendants will have an opportunity to make appropriate objections to a hit including for: 1) privilege; 2) personal in nature (provided no Middesk documents or information is contained within the personal document). Defendants will also have an opportunity to mark hits as HIGHLY CONFIDENTIAL INFORMATION.
- 6) The Forensic Examiner will also have the ability the ability to search for suspicious activity, such as deleted items, USB devices connected to a device or anything else that they deem will be worthy of the report.

WHEREAS, by Thursday April 24th, Defendants Baselayer and Awad have had all the Devices imaged, and all Devices ordered above not previously imaged must be imaged within five (5) business days of the date of this order;

WHEREAS, on Wednesday April 23rd, Plaintiff Middesk provided the Search Terms/Search List to Defendants;

WHEREAS, in addition to the terms above which were ordered by the Court the Court also orders the following:

Preparation for Inspection

1. Prior to imaging any Devices, Forensic Examiner will follow industry standards to properly intake evidence to include, as applicable, recording the evidence make, model, serial number, volume serial numbers, and shall be allowed to take appropriate digital photographs to document their current physical condition and operability. Prior to imaging devices, Forensic Examiner shall properly prepare suitable forensic storage media, including but not limited to an E01/AFF4 Forensic Image File ("Forensic Image File") for receipt of any forensic images created through Forensic Examiner's execution of any directives under this protocol. As part of the Forensic Image File, the Forensic Examiner shall also utilize all other appropriate storage media necessary to appropriately store the applicable data, such as Cellebrite UFDR, native email collection such as Mbox or .pst, etc. Forensic Examiner shall provide the parties with a chain of custody form listing the evidence received, as described within this paragraph.

Imaging of Device(s)

2. Forensic Examiner shall prepare the Forensic Image File. Forensic Examiner shall document and record on an acquisition form: (i) a general description of the process and tools utilized to conduct the imaging; (ii) the MD5 hash value of the original source Device; and (iii) the MD5 hash value of the copy.

3. If any Devices are computers, Forensic Examiner shall also obtain complementary metal oxide semiconductor (CMOS) date and time data within the computer basic input/output system (BIOS). The BIOS date and time should be compared with the actual date and time, and the two shall be recorded.

If any Devices are virtual repositories, Forensic Examiner shall document any and all information necessary to identify the original source of the virtual repositories on the chain of custody form. In addition to the actual data from virtual repositories, Forensic Examiner shall collect independent auditing activity, or logging. Such examples may include Microsoft 365 Enterprise, Google Workspace, Dropbox (commercial or free, but auditing may vary), OneDrive (free version), Google Drive (free version).

4. Forensic Examiner shall be entitled to make additional copies of any forensic image created under this Protocol for purposes of redundancy and disaster recovery.

Preparation for Review and Search of Images

5. Prior to the Forensic Examiner conducting any forensic analysis/examination (a "Review") of any forensic image created from a Device, Forensic Examiner shall ensure that all partitions are displayed/recovered and shall then execute general preparatory actions, including but not limited to: the recovery of deleted folders and files (including from volume shadow copies), OCRing images as applicable, indexing the data, and other actions the Forensic Examiner deems appropriate to assist in the execution of this protocol.

Search for Plaintiff's Data and for Data Search Terms and Reporting Requirements

6. Forensic Examiner shall conduct a search across all Documents, including, but not limited to files and emails on the Devices that are hits to "Plaintiff's Data Search Terms," which may include search terms, MD5 hash values, and/or file names. Plaintiff, through its counsel, will provide Plaintiff's Data Search Terms to the Forensic Examiner before he or she conducts the search. Additional search terms, or iterations of search terms may be agreed upon by the parties. For avoidance of doubt, all searches shall be run against not only all data content, but also against all available metadata fields.¹

7. Following identification of hits responsive to searches executed under the Forensic Examiner's search for Documents and files under "Plaintiff's Data Search Terms" as described in Section 7 above, the Forensic Examiner shall record in a log (the "Hit Log"), any Documents, files and emails (and attachments) that were responsive in either as data content, or within a metadata field, under each of the various searches. Such log will be provided to counsel for the Parties and shall be marked as HIGHLY CONFIDENTIAL INFORMATION pursuant to the Protective Order entered into between the Parties. The log shall, if natively available or otherwise readily accessible, contain the following information about each file: File Name, Document Author, Document Last Saved Author, File Extension, File Size, File System Created / Last Written / Last Accessed / Entry Modified Date, Document Last Printed Date, Document Last Modified / Last Saved / Last Written Date, MD5 hash, Full Path values, Password Protection Status (yes or no), and File Description (archive, file, deleted, overwritten, etc.).

8. The Forensic Examiner shall provide a report showing the following minimum information:

- a. A listing of the make/model/serial number of each and every Device which the Forensic Examiner examined/analyzed, and its storage media within.
- b. A report referencing all removable storage Device(s) turned over for inspection, including:
 1. Date and time the Device was formatted;

¹ The terms "**Document**" or "**Documents**" are used herein in the broadest sense and include, but are not limited to, all original and non-identical copies of the following: all agreements, communications, data, correspondence, telegrams, telegraphs, newspaper or journal articles, excerpts, telexes, text messages, memoranda, electronic mails, emails, electronic files or files, electronic records, books, summaries of records, notices, charts, graphs, maps, blueprints, diagrams, reports, notebooks, plans, surveys, plats, calculations, drawings, sketches, indices, pictures, audio or video tape recordings, accounts, calendars, telephone message logs, e-mail, computer generated messages or data (and all back-up files, tapes and stored memory), including those sent and received on LinkedIn, Facebook Messenger, and Salesforce.com, and any other social media site, schedules, spreadsheets, diaries, journals, opinions, appraisals, drafts, ledgers, receipts, check stubs, and any other paper or writing or document of any kind, character or description (or any summaries thereof), in any form, including paper or electronic.

2. Hardware serial number;
 3. Volume serial number;
 4. Make/model/capacity of Device; and
 5. Identifying information such as the presence of Mac trashes folder or Windows Recycle Bin.
- c. A USB device history report, to include entries from Setupapi logs, registry entries for USBStor and DevClass, logs, Unified Logs, FS Events, Favorite Volumes, Com.apple.finder.plist files, or any other applicable location, for all devices inserted.

9. The Parties acknowledge that the Hit Log shall be supported by additional reports and analysis as described below in Sections 10-15. Such reports and analysis shall pertain solely to the search terms within Plaintiff's Data Search Terms and shall not be conducted on any other files or information on the Devices, except as may be explicitly provided below.

10. As it relates to the items reflected in the Hit Log, the Forensic Examiner shall prepare a report reflecting a non-content full file listing of the contents of the Hit Log for each Device (including all active and deleted files), which includes, if natively available, File Name, Author, File Size, Password Protection Status (yes or no), file metadata including the dates and times for File Created, Last Written, Date Added, File Description (archive, file, folder, overwritten, deleted, etc.) Last Accessed, and Full Path values.

11. In addition to the searching above, the Forensic Examiner shall perform additional review to support the creation of various forensic reports. These reports are exclusive from, and in addition to the searches described above

12. As it relates to the items in the Hit Log, the Forensic Examiner shall create a report listing any and all Desktop/Laptop/Server/NAS/SAN/USB, or any other storage locations and accounts used by Defendants. This report(s) shall include a sequential reference/record number so that parties can refer to a given line item when communicating, and at a minimum:

- a. Full list of file/folder opening artifacts (e.g., lnk, jmp, office mru, recent docs, open save mru, shellbag, etc) created or last written that point to files located on the Device hard drive, or any other location the file opening artifact references (e.g. removable device, network, etc.);
- b. Internet history report for files accessed as well as files being downloaded/uploaded via cloud storage locations including but not limited to Box, Dropbox, YouSendIt, SugarSync, Google Drive, OneDrive, iCloud, etc.;
- c. A listing of all files printed from Defendants' computers or phones, including, where available, File Name, Author, File Extension, File Creation / Last Modified / Last Accessed, MD5 hash and Full Path values;

13. To the extent not already reflected in the Hit Log, the Forensic Examiner shall create a report which fully lists all emails sent or received that are returned as hits in the Hit Log. This report shall list, for each email, the date, time, From, To, CC, BCC, Subject, and Filename(s) of all attachments (to the extent not already include in the Hit Log).

14. As it relates to the items in the Hit Log, the Forensic Examiner shall consider transaction logs and other system files that may contain information to support the reporting requirements above, or in support of other tasks throughout the protocol (e.g., USNJ, VSCs, PLISTs, etc).

15. As to all hits on the Hit Log from smart phones and smart tablets, a Cellebrite or equivalent report of all messages sent or received through any app on such Device (including social media apps, LinkedIn, WhatsApp, etc.), or hits on the Hit Log regarding call logs, voicemail, or contacts, the Forensic Examiner shall provide a report showing:

- a. As to all smart phones and smart tablets, a call log listing all incoming and outgoing calls from December 2022 to the present, including the name of the person on the other line (if known based on existing contacts), phone number, date of the call, time of the call (in UTC) –, duration of the call, whether it was incoming or outgoing.
- b. As to all smart phones and smart tablets, a listing of all voicemails received and saved on the Device from December 2022 to the present, including the name of the caller who left the voicemail (if known), phone number of the caller who left the voicemail, date the voicemail was received, time the voicemail was received and duration of the voicemail.
- c. As to all smart phones and smart tablets, a listing of all Contacts saved on the phone, including name, company name, all phone numbers, email addresses, physical addresses, and any other notes retained about the individual, as well as metadata associated with each contact, including the date the contact was created on or added to the phone.

16. Forensic Examiner shall conduct additional analysis for information relevant to the identification, use, disclosure, transfer, access, deletion, or destruction of potentially relevant data as may be directed by the Parties or the Court.

17. Forensic Examiner shall provide copies of the reports described in this section to counsel for the Parties. The reports shall be treated in a confidential manner and can be used in court provided that they are filed under seal unless the Parties agree otherwise. The reports may be shared by counsel with all Parties, including as to Plaintiff Middesk, to the appropriate management representatives of the corporate party who have need to access this information for purposes of prosecution of this case.

Access to Files

18. The Forensic Examiner shall provide access to the data responsive to Plaintiff's Data Search Terms as follows. Defendants' counsel will have seven (7) business days after receipt

of the Hit Log, of the documents in a form that can be reasonably reviewed, and all other reports and data from the Forensic Examiner to review and specifically identify to Plaintiff's counsel any objections to the items contained in the Hit Log or the accompanying reports. Defendants' counsel shall not designate as privileged any of Plaintiff's alleged property ("Plaintiff's Documents"), including its alleged Confidential Information or any evidence, including relevant metadata, of use, disclosure, access or destruction of Plaintiff's files or information.

19. Plaintiff's counsel and those individuals who may have access to information designated as CONFIDENTIAL INFORMATION or HIGHLY CONFIDENTIAL INFORMATION, as applicable, pursuant to the Protective Order will have immediate access only to those files responsive to Data Search Terms that Defendants' counsel does not object to within seven (7) business days after receipt of the Hit Log and all other Forensic Examiner reports². Once Defendants' seven (7) business day deadline to make objections has expired, Plaintiff's counsel shall be provided access to all search term responsive data Defendants' counsel has not identified as privileged or subject to another valid objection that would remove it from the production. Nothing in this Protocol shall be deemed to limit the proper scope of discovery or prevent a party from seeking relevant documents through proper discovery requests.

20. Counsel for the Parties will meet and confer regarding the disposition of any files where there is a dispute concerning the proper owner or relevance, or the removal from production, as well as the disposition of Plaintiff's files or other documents belonging to Plaintiff in Defendants' possession. To the extent the Parties are unable to resolve any dispute over Defendant's objections or the ownership of any files or relevance, the Parties agree that the dispute may be resolved by the Court but the confidentiality of said files shall be maintained during the period of the Parties' dispute and subject to either Parties' right to seek additional protections for the files.

Other Analysis

21. **Deleted File Analysis** – The Forensic Examiner is also authorized to analyze any documents that may have been or were deleted from December 2022 through the present (the "Relevant Time Period") to identify, to the extent possible, the date and time such Documents were deleted, the contents of the deleted Documents, and metadata identifying the date the Documents were created, last accessed, last modified, and any other attributes available regarding the Documents. If any such deletion activity is found to have occurred, the Forensic Examiner shall provide a summary of this activity in a written summary report (the "Report").

22. **Anti-Forensic Evaluation** – The Forensic Examiner shall conduct reasonable searches for and evaluate if any anti-forensics evidence elimination techniques were employed such as: (1) evidence of searches for deleting files or removing content, (2) evidence of search for or purchases of software to delete files or remove content, (3) evidence of running software

² For any objections to the files or data, for which Defendants have legitimate grounds to exclude from the production based on the text of this Order, Defendants shall provide a log of files that are removed from the production / review and must include, to the extent available, the verbatim name of the file, verbatim subject of the email or document, date, each sender and recipient, and the reasons for the document being excluded from the production.

designed to delete files or remove content, (4) evidence of clearing of browsing history, (5) evidence of running shell commands or scripts in Terminal or equivalent application, which would include the listing of these commands, (6) evidence of items in Trash /Recycle Bin or clearing of Trash/Recycle Bin, (7) evidence of changing retention settings on mobile devices, and (8) any other analysis the Forensic Examiner deems necessary through its expertise; after reviewing this information, the Forensic Examiner will report to the Parties, in writing, whether any anti-forensics evidence elimination techniques were employed, and if so, details must be provided in the Report. The report shall also include, to the extent detected from the evaluation above, information related to the download, purchase, installation, execution, usage, or removal of any data wiping, obfuscation, anti-forensics or time stamping, including specific information on the source, usage, and extent of any files permanently unavailable/irrecoverable following the use of any wiping or remediation software.

23. **External Storage Device History Reconstruction** – The Forensic Examiner shall reconstruct and describe in the Report any external storage device use by creating an inventory of all USB flash drives and external hard drives that were attached to the Electronic Devices during the Relevant Time Period, along with the dates such devices were attached, associated time stamps, their serial numbers, and whether there is any evidence of the transfer of Documents to or from the external storage device.

24. **Review of Photographs and Images** – The Examiner shall OCR photographs and images found on the devices to allow for searching before running search terms and preparing the Hit Log so those can be included in the search.

Return of Original Device(s)

25. Upon completion of the Imaging, Forensic Examiner shall return the Devices, but the Devices shall be subject to remediation, if applicable, as agreed upon by the Parties. Logistics for how to remediate the Devices shall be agreed upon by the Parties once the review has been completed. On a case-by-case basis, the Parties may agree that the device(s) may be held by the Forensic Examiner until remediation takes place.

Remediation

26. Counsel for the Parties shall meet and confer concerning the extraction and removal of Plaintiff's files from the Devices after the reports are received and any disputes are promptly resolved. The Parties will identify the data to be deleted and the Forensic Examiner will permanently delete from the Devices all Plaintiff's alleged property that is found on the Devices, including its alleged Confidential Information, subject to the Parties' mutual agreement regarding scope and timing. Logistics for how to remediate the Devices shall be agreed upon by the Parties once the review has been completed. The Forensic Examiner shall retain a forensic image of all the Devices for preservation purposes for the duration of this litigation.

Right to Supplement

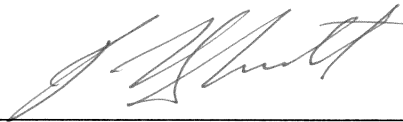
27. Based on the results of this executed Protocol, and any new additional information obtained during the execution of this Protocol, the Plaintiff reserves the right to request additional analysis on the devices covered within this Protocol.

Protocol Period

28. This Protocol shall be effective beginning on the date it is ordered by the Court and will continue until the remediation in Section 27 is completed (the “Protocol Period”).

IT IS SO ORDERED.

Dated: May 13, 2025



Hon. P. Kevin Castel, U.S.D.J.